DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

MICHELLE J. KANE (CABN 210579)
KATHERINE L. WAWRZYNIAK (CABN 252751)
Assistant United States Attorney

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (510) 637-3680
FAX: (510) 637-3724
michelle.kane3@usdoj.gov
katherine.wawrzyniak@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. YEVGENIY ALEXANDROVICH NIKULIN, Defendant.	No. CR 16-00440 WHA **UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION UNDER RULE 29 FOR A JUDGMENT OF ACQUITTAL NOTWITHSTANDING THE VERDICT AND, ALTERNATIVELY, MOTION FOR A NEW TRIAL UNDER RULE 33** Date: September 29, 2020 Time: 2:00 p.m. Courtroom 12, 19th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Federal Rules

INTRODUCTION

Defendant's motions for acquittal and for a new trial focus entirely on questions of credibility and weight. These are questions for the jury to resolve, and the jury has done so in the form of guilty verdicts on each count.

In its focus on the jury's evaluation of evidence admitted at trial, the defendant's brief in support of its motion for acquittal is an implicit admission that there was sufficient evidence to support each verdict, and amounts to a request that the Court reevaluate that evidence in the light most favorable to the defense, something the law does not allow. The government has offered evidence in the form of testimony, recordings, and documents to support a jury verdict of guilty on each count of the Indictment. Resolving all conflicts in favor of the prosecution, there are no grounds to grant defendant's motion.

Moreover, even under the broader examination permitted for a new trial motion, the weight of the evidence is on the side of the jury's guilty verdicts. A fair review shows that the verdicts reflect the most reasonable conclusion in light of all the evidence introduced by the government. Defendant cannot establish that allowing the verdicts to stand will create a miscarriage of justice that would merit throwing out the jury's carefully considered verdicts and returning for a new trial before a new jury.

BACKGROUND

On July 10, 2020, after a seven-day trial, a jury found defendant Yevgeniy Alexandrovich Nikulin guilty on all nine counts of the Indictment. ECF No. 259 (Special Verdict Form). The jury also agreed that the government had proven at least one aggravating factor increasing the maximum penalties for Computer Intrusion in violation of 18 U.S.C. § 1030(a)(2) from one year of imprisonment to five years for Counts One, Four, and Seven, and increasing the maximum penalties for Causing Damage to a Protected Computer in violation of 18 U.S.C. § 1030(a)(5)(A) from one year of imprisonment to ten years for Counts Two and Eight. The jury found only one of two possible aggravating factors for Counts Four (Computer Intrusion in violation of 18 U.S.C. § 1030(a)(2) as to Dropbox) and Seven (Computer Intrusion as to Formspring).

On August 25, 2020, defendant moved for acquittal as to all counts pursuant to Fed. R. Crim. P. 29(a) and for a new trial pursuant to Fed. R. Crim. P. 33. Rule 29(a) applies to motions before submission to the jury. The Court deemed defendant to have made a Rule 29 motion at the close of the

government's case on July 9, 2020, and, pursuant to Rule 29(b), the Court reserved decision until after any jury verdict. Trial Transcript ("Trial Tr.") at 867: 23-25. On July 10, 2020, following the jury's verdict, defendant requested, and the Court tentatively allowed (subject to the submission of a stipulated briefing schedule) an extension for the deadlines to file a Rule 29 or Rule 33 motion so that the motions could be heard at the sentencing hearing. Trial Tr. at 1005:18-24.[1]

ARGUMENT

I. The Court Should Deny Defendant's Rule 29 Motion

A. Standard for a Rule 29 Motion for Judgment of Acquittal

The Supreme Court and Ninth Circuit have held that when considering a motion for acquittal under Fed. R. Crim. P. 29, "the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979) (emphasis in original); *see also McDaniel v. Brown*, 558 U.S. 120, 132 (2010) (reaffirming this standard); *United States v. Miller*, 953 F.3d 1095, 1108 (9th Cir. 2020); *United States v. Dreitzler*, 577 F.2d 539, 545 (9th Cir. 1978) ("It is well settled that a district court does not have unlimited discretion in resolving a Rule 29(c) motion for judgment of acquittal. Rather, the district court must determine 'whether at the time of the motion there was relevant evidence from which the jury could reasonably find [the defendant] guilty beyond a reasonable doubt, viewing the evidence in light favorable to the government.'") (quoting *United States v. Figueroa-Paz*, 468 F.2d 1055, 1058 (9th Cir. 1972)).

In ruling on a Rule 29 motion, the district court's "function . . . is quite narrow" and it must bear in mind that it is the "jury's exclusive function to determine the credibility of witnesses, resolve evidentiary conflict and draw reasonable inferences from proven facts." *United States v. Bernhardt*, 840 F.2d 1441, 1448 (9th Cir. 1988); *see also United States v. Sherwood*, 98 F.3d 402, 408 (9th Cir. 1996) (rejecting challenge to sufficiency of evidence where defendant's sole argument was credibility of the witnesses implicating him). "Circumstantial evidence and inferences drawn from it may be sufficient to sustain a conviction." *United States v. Jackson*, 72 F.3d 1370, 1381 (9th Cir. 1995) (citation omitted);

[1] On August 6, 2020, the Court entered a modified briefing schedule setting August 25, 2020, at noon as the deadline for defendant's motions. ECF No. 267.

see also United States v. Grasso, 724 F.3d 1077, 1086 (9th Cir. 2013) (finding circumstantial evidence and inferences drawn from that evidence sufficient to support conspiracy conviction).

In making this determination, the evidence and all the inferences from the evidence must be viewed in the light most favorable to the Government; the defendant bears a heavy burden. *See Glasser v. United States*, 315 U.S. 60, 80 (1942); *see also United States v. Nevils*, 598 F.3d 1158, 1164 (9th Cir. 2010) (en banc) ("We reject [defendant's] invitation to construe the evidence in the light most favorable to his claim of innocence, because such an approach is foreclosed by *Jackson*."). On a motion for acquittal, the court must consider that it is "the exclusive province of the jury to determine the credibility of witnesses, resolve evidentiary conflicts, and draw reasonable inferences from proven facts, by assuming that the jury resolved all such matters in a matter which supports the verdict." *United States v. Stewart*, 420 F.3d 1007, 1015 (9th Cir. 2005) (citations omitted). The relevant inquiry is not whether the evidence excludes every hypothesis except guilt, but whether the jury could reasonably arrive at its verdict. *United States v. Aichele*, 941 F.2d 761, 763-764 (9th Cir. 1991); *United States v. Mares*, 940 F.2d 455, 458 (9th Cir. 1991).[2] Applying this standard, the Court should deny the motion for acquittal on all counts.

B. The Jury Rejected Defendant's Baseless Challenges to FBI Special Agent Jeffery Miller's Credibility

Defendant argues that "contradictions and inaccuracies" in FBI Special Agent Jeffrey Miller's testimony made him not credible, but does not point to any specific contradiction or inaccuracy. Instead, defendant argues, as defense counsel did in closing, that Special Agent Miller was biased and therefore unreliable. At trial, defendant cross-examined Special Agent Miller at length regarding an unrelated alleged cybercriminal. Special Agent Miller testified as to how he conducted his investigation and why he did not have any reason to suspect that person in the charged crimes. Defendant then argued that the FBI should have pursued that individual and that the jury should therefore find Special Agent Miller biased and unreliable. In reaching its verdict, the jury rejected this assessment of Special Agent Miller, because there was no basis for it.

[2] The standard is the same for denial of a motion for judgment of acquittal as for a challenge to the sufficiency of the evidence following conviction. *United States v. Shirley*, 884 F.2d 1130, 1134 (9th Cir.1989).

A significant element of the defense in this case was an attempt to suggest that an alleged Russian cybercriminal named Evgeniy Bogachev could have been responsible for the charged offenses. None of the evidence – none of the online accounts, videos, recordings, victim logs, or other items – pointed to Evgeniy Bogachev. Instead, defendant cross-examined Special Agent Miller on Bogachev and put into evidence an FBI "wanted poster" describing allegations against Bogachev in connection with various U.S. indictments. This was all done in furtherance of suggesting that Bogachev could have committed the crimes for which defendant was convicted, and that Special Agent Miller's investigation was deficient because he should have focused on Bogachev due to his having the same first name as defendant.

During his direct testimony, Special Agent Miller walked methodically through his investigation. This included an explanation of when he first became aware of defendant's name through receiving Russian ISP records discussed in more detail below. Trial Tr. 462:24-463:3. Special Agent Miller told the jury how, at the time he made the request to Russia for ISP records of the subscribers assigned the IP addresses used in the LinkedIn intrusion, he had also been pursuing a different lead – that is, Alexey Sipkin, the individual who had posted a portion of the hashed LinkedIn passwords on a Russian internet forum. Trial Tr. 464:24-466:1. Overall, Special Agent Miller's testimony on direct examination established that he followed many leads in the investigation that he was not able to resolve but that did not point to defendant. None of the leads he described on direct examination involved the name Evgeniy Bogachev.

On cross-examination, defense counsel raised the name Evgeniy Bogachev by questioning Special Agent Miller about a wanted poster naming him. Trial Tr. 690:15-695:6. Defense counsel specifically questioned Special Agent Miller about the "Gameover Zeus" botnet that Bogachev was accused of using. In response to cross examination questions, Special Agent Miller made clear that he did not start or conduct his investigation by looking for evidence of involvement by known Russian cyber criminals. He instead testified that he followed the evidence that he developed through his own investigation and pursued the leads to specific individuals that way. Trial Tr. 689:15-690:11. Defense counsel further pushed Special Agent Miller on purported similarities between Bogachev and defendant. Trial Tr. 720:12-733:1. At one point, Special Agent Miller explained, "There are a lot of individuals

who hack companies, but you have to follow the evidence. So you just can't say: Yes, he is Russian and he has the same first name." Trial Tr. at 731:17-19. He testified that he would look at other FBI investigations of cyber criminals if the evidence in his own investigation led there. Trial Tr. 720:12-733:1. Special Agent Miller testified again that he had identified and investigated other individuals in addition to defendant. Trial Tr. 688:13-21. He also said that he found no evidence pointing to involvement by Evgeniy Bogachev. Trial Tr. 729:4-730:1. Specifically, he stated, "What I will say is during my investigation, yes, there was the name Yevgeniy. And I followed the evidence and – and let it lead where it led. Followed every thread. At no point during my eight-year investigation did I find any ties to Mr. Bogachev." Trial Tr. 729:11-15.

Defendant also argues in his brief, without any support, that Special Agent Miller was not qualified to testify on the subject of cybercrime because of his alleged lack of familiarity with known cyber criminals. The only evidence in the record was that Special Agent Miller was familiar with the individuals relevant to his investigation, including defendant's co-conspirators. *E.g.*, Trial Tr. 687:21-688:12. Moreover, the government provided notice of Special Agent Miller as an expert on computer forensics and the market for, and uses of, stolen credentials. ECF 125. That notice included a summary of his qualifications, which the government also put into evidence through his testimony. Trial Tr. 411:5-415:19; 623:11-23. There was no claim that Special Agent Miller was familiar with the name of *every* cyber criminal in the world or even *every* Russian cyber criminal, and the fact that he might not be did not undercut his expertise at all. Defendant did not challenge Special Agent Miller's qualifications to testify regarding criminal underground markets either before or during trial.

Defendant's claim about Special Agent Miller's testimony regarding Bogachev amounts to a complaint that the FBI failed to "round up the usual suspects,"[3] exactly the type of thing that law enforcement agencies are not supposed to do. Special Agent Miller's testimony established that he instead did what he *was* supposed to do: "follow the leads in the case." Trial Tr. at 690:4-11. Defense nevertheless argued in closing that Special Agent Miller was not credible because of his bias. Trial Tr. 958:13-960:15. This argument found no traction because it was not tied at all to actual evidence before

[3] *Casablanca*, Warner Bros. 1942.

the jury, which instead established that the FBI's investigation was methodical, reasonable, and thorough. It was the jury's job to weigh the credibility of witnesses, and they clearly found Special Agent Miller credible.

C. The "Hotel Videos" Provided Evidence Linking Defendant to his Co-Conspirators and to Oleksandr Ieremenko

The United States introduced Exhibit 74, a video and audio recording obtained from Oleksandr Ieremenko's computer of defendant at a Moscow hotel in March 2012 with co-conspirators including Nikita Kislitsin and Oleg Tolstikh. The video showed defendant mugging for the camera and making an obscene gesture. The translated audio established that the group had the following discussion:

Male Speaker l: Put computers in circles.

Male Speaker 2: How many people are there in this city?

Male Speaker 1: 30 thousand.

Male Speaker 2: 30 thousand. One Internet cafe.

Male Speaker 1: One Internet cafe. A person can come for free, surf the Internet, maybe order a cup of tea.

Male Speaker 3: Look, I know this city very well, my brother lives there. If you provide free Internet in such an ass of the world...

Defendant argues in his brief, as defense counsel did at closing, that this is "guilt by association" and claims that this discussion is about the development of a potential internet café. Trial Tr. 952:16-953:10. He is wrong on both claims.

Defense counsel questioned Special Agent Miller about the defense theory that this meeting was about a legitimate business plan. He observed in response, "I haven't been in many business meetings where someone gives the bird to others laughing and joking." Trial Tr. 686:16-687:10. Moreover, the plain language of the transcript does not support the conclusion that the people at the meeting are starting a business. It is unclear what the point of the conversation is, other than that they are discussing Internet access in a Russian city. This video is direct and highly relevant evidence that connects defendant to two of his co-conspirators in a discussion about the Internet just months before he hacked Formspring and then worked with two of the men pictured in the video to sell the stolen data.

The government also introduced Exhibit 72, a video taken earlier the same day and found on the same computer, in which Oleksandr Ieremenko is filming while a passenger in a car driven by an unnamed individual who also appears in the hotel meeting video at Exhibit 74. At the end of Exhibit 72, a black car pulls in front of the car in which Ieremenko is riding. Exhibit 66D was a photograph, also from Ieremenko's computer, of defendant driving what appeared to be the same car, as identified by the color and make by Special Agent Miller. Trial Tr. 642:21-643:14; 649:22-650:2.[4]

Defendant argues that the video at Exhibit 72 does not connect defendant to the charged intrusions, but in fact, the video does just that, in a small but important way: in combination with the photo at Exhibit 66 there is a reasonable inference of a pre-existing friendship between defendant and Ieremenko that makes it more likely that the "Yevgeniy Lomovich" who sent Ieremenko stolen LinkedIn data later in 2012 was in fact defendant. The jury could have reasonably inferred from the nature of the interactions and the defendant's attitude in the Exhibit 74 video that defendant knew Ieremenko well enough to be the person who casually shared stolen data alongside a discussion of his love life and impending birthday. The fact that defendant had the stolen LinkedIn data in October 2012, when it was not otherwise public, could, in combination with other evidence, lead the jury to conclude that the defendant committed the LinkedIn intrusion.

D. The Jury Found the Subscriber Records Reliable

In his brief, defendant attacks the jury's consideration of the subscriber records from Russian National Cable Networks ("NCN"), showing that as of March 3, 2012, defendant was the registered subscriber for the IP address ending in .239, which the government obtained via a mutual legal assistance treaty ("MLAT") request to the Russian government. This argument is not well founded for two reasons. First, defendant failed to file a motion opposing admission in evidence of such records before trial. Therefore, his objection is waived. Second, notwithstanding defendant's failure to timely object to the evidence, defendant argued the unreliability of the records to the jury, and the jury nevertheless reasonably relied on the records.

//

[4] Defendant concedes in his brief that it was him driving the black Bentley in the video.

The admissibility of foreign business records in a criminal proceeding is governed by statute, 18 U.S.C. § 3505. Subsection (a) provides that a foreign record of regularly conducted activity shall not be excluded as hearsay if it is accompanied by a foreign business records certification. Subsection (b) requires the proponent of the evidence to provide written notice of its intention to introduce the records. The opposing party must file any motion opposing admission before trial. "Failure by a party to file such motion before trial shall constitute a waiver of objection to such record or duplicate, but the court for cause shown may grant relief from the waiver." 18 U.S.C. § 3505(b).

Here, the government provided ample advance written notice of its intent to introduce the subscriber records at trial. The records were listed in the government's first filed exhibit list (ECF 123, filed December 4, 2019), and the subsequent exhibit lists filed before trial (ECF 162, 175). On February 26, 2020, AUSA Kane sent an email message to defense counsel listing the records that the government intended to authenticate at trial with custodian certifications, specifically including the Russian/NCN subscriber records. Defense counsel did not raise any concerns in pretrial communications regarding authentication of the records. The government's Trial Brief, filed March 3, 2020, specifically addressed the admissibility of the records under Section 3505. *See* ECF 170, at 7-8. Despite multiple opportunities to do so, defendant never raised any issues with the records or the foreign certification before trial. In fact, defendant stipulated to the accuracy of the English translation of the MLAT response. ECF 178, ¶ 14. Under the plain language of the statute, defendant waived his objection.

At trial, the government moved the MLAT response and the English translation, Exhibits 85 and 85A respectively, into evidence during Special Agent Miller's direct examination. Defense counsel orally affirmed the stipulation to the accuracy of English translation, and both documents were received into evidence without objection. Trial Tr. 450:17-451:23. A short time later, the government moved the foreign certification, Exhibit 86, into evidence, again without objection. Trial Tr. 461:6-22. Thus, the documents defendant now challenges were properly admitted.

During cross-examination of Special Agent Miller, defense counsel displayed the foreign certification again and pointed out that E.S. Karpushkin, the person who had completed it, had not filled in the blanks for his position and employer. Trial Tr. 769:18-771:15. Defense counsel also made the point that any information received from the Russian government should be viewed with skepticism.

Trial Tr. 773:15-20. Special Agent Miller pointed out that each page of the MLAT response from Russia bore stamps indicating it was verified. Trial Tr. 771:20-772:10. He also spoke about his regular reliance on evidence obtained through MLAT requests in his investigations. Trial Tr. 772:20-774:8. Then on re-direct, the government established that it was common for Russians to use initials for the first and second names in a signature, as indicated in other places within the MLAT response. Trial Tr. 854:1-4.[5]

On this record, it is apparent that the jury had the opportunity to consider defendant's arguments regarding the source of the Russian subscriber records and the alleged deficiencies[6] with the foreign certification. It was not unreasonable for the jury to reject or discount those arguments, particularly given the other evidence in the case, obtained through other means, linking defendant to the Kantemirovskaya Street address that appears in Exhibit 85A.

E. The Jury Rejected the Implausible "Other Evgeniy" Defense

As discussed above, defense counsel cross-examined Special Agent Miller about an individual named Evgeniy Bogachev.[7] Part of that questioning used an FBI wanted poster to elicit facts about Bogachev that were framed as similar to defendant – Bogachev shared a first name with defendant, was from Russia, and had been accused of cyber crimes. Trial Tr. 729:4-733:1. Defense counsel later argued those facts about Bogachev in closing. Trial Tr. 959:1-8. The jury clearly did not find merit in the implausible suggestion that simply because there is another Russian cyber criminal named Evgeniy that all of the government's evidence pointing to defendant was suspect. Moreover, as Special Agent Miller noted, there was no evidence that Bogachev himself was a hacker. Trial Tr. 731:20-732:2. In addition to

[5] The government also showed the jury a cover letter from Department 5 of the Control and Methodology Directorate of the Main Investigative Directorate of the Main Directorate of the Ministry of Internal Affairs of the Russian Federation for the city of Moscow, included with the MLAT response indicating it had been prepared by E.S. Karpushkin; the reasonable inference is that Karpushkin was an official of the Ministry. Exh. 85A; Trial Tr. 851:25-853:25.

[6] Exhibit 86 meets the definition of a foreign certification in 18 U.S.C. § 3505(c)(2); that is, it was signed in a foreign country by a qualified person; it clearly recites the business records requirements, and it states that the signer would be subject to criminal penalty in Russia for a false declaration. To the extent that the title and employer of E.S. Karpushkin is not provided, this is a technical deficiency that goes to the weight, not the admissibility, of the underlying evidence. *See generally United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988) (question as to accuracy of certain business records affected only their weight, not their admissibility).

[7] Testimony by Russian linguist established that Yevgeniy and Evgeniy are alternate English renditions of the same Russian name. Trial Tr. 360:6-12.

failing to dent Special Agent Miller's credibility through the claim that he failed to investigate Bogachev because of bias, the defense failed to convince the jury that any other cyber criminal could have committed the charged crimes. Defendant asked the jury to speculate as to a possible role for a different Russian man where there was absolutely no evidence tying him to the offenses. The jury rejected the argument and the Court should too.

F. The Recorded Calls Allowed the Jury to Hear Defendant in his Own Words

At trial, the government introduced five recorded calls and their English language translations featuring defendant speaking from jail to friends and family. [8] Anticipating that defendant was mounting an identity defense, the purpose of putting the calls in evidence was to use defendant's own words to link him to evidence associated with the charged intrusions, to let the jury hear his references to "hacking," and to establish defendant's ongoing interest in high tech subjects:

- The call at Exhibit 88 established that Defendant's family received mail at an address Kantemirovskaya Street. Other evidence in the case showed that chinabig01@gmail.com and r00talka@gmail.com had both searched for Kantemirovskaya Street. As discussed above, the Russian NCN subscriber records for the IP address ending in .239 also showed defendant resided on Kantemirovskaya Street.
- Exhibit 89 contained admissions by the defendant: "I hack websites 24/7. I hacked….I want to hack the prison here [laughing]….I want to hack the prison. The rules here are stupid." This call also established a relationship between defendant and Anna Shvedova, a/k/a Anya, whom dex.007 referenced in Skype chats with Ieremenko.
- Exhibits 90, 135, and 136 evidenced defendant repeatedly asking for reading material about technology—computers, the new iPhone, "what happens in the modern world." These calls showed defendant's continued interest in technology, undermining defendant's argument that he was an innocent nobody framed by the Russian government.

As the government had argued in its Trial Brief, the calls were admissible under Fed. R. Evid. 801(d)(2)(A). (*See* ECF 170, at 8.) Moreover, the calls were relevant, under Fed. R. Evid. 401, to the

[8] Due to technical difficulties playing the Russian audio of the calls over Zoom, the government read the English transcripts of the calls into the record.

core issue of identity. In Exhibit 89, defendant referenced his custodial status. The reference is inextricable from the admission ("I want to hack the prison"). In Exhibit 136, defendant referred to asking "the guards" for something, an indirect reference to his custodial status.

Between January and July 2020, government counsel corresponded with defense counsel multiple times via email and phone about the jail calls—the government's intention to use them; their translations; how they would be clipped. Apart from refusing to agree to the translation of "hack" [9] in Exhibit 89, defendant did not raise any objections to the calls or translations. He stipulated to the introduction of the translations at Exhibits 88, 90, 135, and 136. Defendant also did not move to exclude the calls via motion *in limine*. Nor did he object when the calls were offered in evidence on July 7, 2020. Trial Tr. 502:16-505:14.[10]

After government counsel read Exhibit 89, and again after government counsel read Exhibit 136, the Court gave an immediate admonition to the jury that they were to draw no inference of guilt from the fact that defendant was ever in custody. Trial Tr. 509:6-16; 515:15-22.[11] On this record, it is clear that the jail calls were offered and admitted for a legitimate purpose—proving identity. The jury could reasonably infer from the content of the calls, alongside other evidence in the case, that defendant was chinabig01@gmail.com, the person who lived on Kantemirovskaya Street in Moscow in 2012, and was responsible for the charged intrusions.

II. The Court Should Deny Defendant's Motion for a New Trial

A. Standard for a Rule 33 Motion for New Trial

Fed. R. Crim. P. 33 provides that "the court may grant a new trial to that defendant if the interests of justice so require." In moving for a new trial, defendant does not raise any issue regarding

---

[9] Certified Russian interpreter Andre Romanenko testified that Exhibit 89 was an accurate translation of the Russian conversation in Exhibit 89A. (Trial Tr. 358:14-359:4.)

[10] At defense counsel's request, AUSA Kane read the stipulation regarding the recordings of the calls for the jury, but did not include a previously-agreed upon reference to defendant being in custody at the time the recordings were made. ECF 178 2:3-6 (Stipulation No. 5), Trial Tr. 503:17-20.

[11] In its presentation of the recordings, the government avoided any explicit questioning or testimony regarding defendant being in custody for any crime. Only on cross-examination did defense counsel ask a series of questions clarifying that defendant had been in pretrial detention at the time the recordings were made and attempting to distinguish between "prison" and "jail" to establish that defendant had not yet been convicted. Trial Tr. 681:20-683:18.

newly-discovered evidence, but instead renews his Rule 29 argument that the evidence was insufficient to support the verdicts. The sufficiency argument is again predicated on a weighing of the credibility and reliability of witnesses and documentary evidence.

In ruling on such a motion, "If the court concludes that, despite the abstract sufficiency of the evidence to sustain the verdict, the evidence preponderates sufficiently heavily against the verdict that a serious miscarriage of justice may have occurred, it may set aside the verdict, grant a new trial, and submit the issues for determination by another jury." *United States v. Kellington*, 217 F.3d 1084, 1097 (9th Cir. 2000) (citations omitted). The Court should grant a new trial "only in exceptional cases in which the evidence preponderates heavily against the verdict." *United States v. Showalter*, 569 F.3d 1150, 1157 (9th Cir. 2009) (quoting *United States v. Pimental*, 654 F.2d 538, 545 (9th Cir. 1981)); *see also United States v. Cutting*, No. 14-CR-00139-SI, 2018 WL 2021224, at *2 (N.D. Cal. May 1, 2018) (denying Rule 29 and 33 motions based on sufficiency of the evidence); *United States v. Hurth*, No. CR 09-292-GAF, 2010 WL 11469809, at *1 (C.D. Cal. Aug. 5, 2010) ("Though stated in broad terms, Rule 33 is not meant as a device through which the Court may substitute its judgment for that of the jury."). Here, the Court should reject defendant's challenge to Special Agent Miller's credibility and to the reliability of the documentary evidence, just as the jury did. Because there is no miscarriage of justice in letting the verdicts stand, the Court should deny the motion for a new trial.

B. The Evidence Strongly Supported the Verdicts

Defendant claims that allowing the verdicts to stand would result in a miscarriage of justice, for the same reasons stated in the Rule 29 portion of the brief. As discussed above, the evidence viewed in the light most favorable to the government supported each verdict. But more than that, the evidence viewed in *any* reasonable light heavily favored the jury's guilty verdicts. Nothing but speculation and baseless attacks on credibility supported defendant's arguments to the contrary. Defendant therefore cannot establish that this is the "exceptional" case in which the Court should grant a new trial.

The evidence showed that, in 2012, LinkedIn, Dropbox, and Formspring all suffered computer intrusions that involved the theft of customer credentials. Defendant concedes as much in his brief. The evidence further established five key propositions leading to the conclusion that defendant was guilty of committing those intrusions: (1) chinabig01@gmail.com was responsible for all three intrusions; (2)

chinabig01@gmail.com was connected to a constellation of other electronic accounts, including r00talka@gmail.com; (3) chinabig01@gmail.com and r00talka@gmail.com were controlled by the same person; (4) r00talka@gmail.com was Yevgeniy Nikulin; and therefore (5) Yevgeniy Nikulin committed the intrusions.

As to the LinkedIn intrusion, the evidence showed that someone targeted LinkedIn Site Reliability Engineer Nick Berry. Once this person had Nick Berry's credentials, he was able to access LinkedIn's corporate network via Virtual Private Network ("VPN"). He eventually was able to log on to a LinkedIn production server using Mr. Berry's credentials and exfiltrate LinkedIn user data. Retired FBI Special Agent Bryant Ling examined Nick Berry's iMac computer and explained how, between February 6 and February 12, 2012, it was compromised. Exh. 131 (summary chart of log entries). He explained that the hacker put a malicious shell called "madnez" on Nick Berry's machine, which allowed someone to send commands to the computer remotely. When launched, the program called itself "!C99madShell v. 2.0 madnet edition!" Exh. 131A (Madnez shell screen shots); Trial Tr. 145:12-146:25; 148:1-149:1; 166:4-171:25.

Bruno Connelly and Ganesh Krishnan of LinkedIn explained that log files showed the intruder posing as Nick Berry and logging on to the LinkedIn VPN. Exh. 33. There was one extremely long VPN connection in the logs, which used a Russian IP addressing ending in .239. Mr. Connelly's testimony was that, while the intruder was logged in through Nick Berry's VPN, he used Nick Berry's SSH key to log into some LinkedIn database machines, including one that ran the Oracle database used to store customer login information. Trial Tr. 57:12-24; 76:25-77:16. Mr. Connelly testified that millions of usernames and hashed passwords were stolen.[12] Trial Tr. 60:25-61.4; 75:5-17.

Mr. Connelly testified that LinkedIn identified approximately 30 people who had unauthorized logins to their accounts from Russian IP addresses, including victims who worked at Dropbox and Formspring. Exhs. 32 and 32A; Trial Tr. 60:8-61:6. This showed the person who committed the LinkedIn intrusion conducting reconnaissance, just as he had with Nick Berry, to find additional targets. LinkedIn identified the unauthorized access to those accounts by linking the Russian IP addresses used

[12] He explained that "hashed" meant that the passwords had been run through an algorithm and did not appear in plain text. Trial Tr. 21:5-22:3.

with Nick Berry's VPN logins to two "browser cookies." Mr. Connelly explained that a browser cookie was a unique string that would identify anything that a particular web browser did on LinkedIn's system, even across different Internet connections. Trial Tr. 48:9-49:9 He also testified that the incident response team found a similar "sputnik" user agent string associated with many of the unauthorized logins. He testified that a user agent string is information about the user's system that a web browser sends to a website. Trial Tr. 49:13-50:15. Both Mr. Connelly and Mr. Krishnan testified that the sputnik user agent string was unusual and stood out. Trial Tr. 50:23-51:6; 293:22-294:8. LinkedIn used the Russian IP addresses, the two suspect browser cookies, and the sputnik user agent string to identify the attacker's activity.

The evidence showed that the Dropbox intrusion began with the use of Tom Wiegand's credentials. Much like Nick Berry, Mr. Wiegand was targeted. He testified that he had a LinkedIn account in 2012, and that at the time, his system was to use the same username and password across his accounts. This meant that, once someone had his LinkedIn username and password, it would have been easy to impersonate Mr. Wiegand on the Dropbox system. Trial Tr. 104:20-105:3. Dropbox determined that the intruder used credentials belonging to Mr. Wiegand and other Dropbox employees to access the Dropbox corporate network from Russian IP addresses. Exh. 142; Trial Tr. 87:3-12.[13] Former U.S. Secret Service Agent Cory Louie of Dropbox testified that the intruder also accessed an internal "wiki" through compromised employee accounts and viewed information on the corporate computer infrastructure. Trial Tr. 92:24-93:16. Eventually, the intruder used Mr. Wiegand's account to invite himself to the Dropbox corporate employee Teams account. Exh. 3C; Trial Tr. 106:10-24; 108:6-109:2. He stole a file that contained a subset of Dropbox usernames and hashed passwords. Trial Tr. 94:10-95:2.

The evidence showed that the Formspring intrusion began with the compromise of John Sanders' credentials. The logs showed that someone logged on to the Formspring corporate network as Mr. Sanders from a Russian IP address. Exh. 19. The intruder then probed the corporate network and used

[13] Mr. Louie testified about how Dropbox identified unauthorized access. For example, he testified that the GVC code, similar to the LinkedIn browser cookie, was a unique string of characters that identified a computer accessing Dropbox, even across different Internet connections. Trial Tr. 90:13-91:9.

SSH to log in to the Formspring development server and exfiltrate the Formspring account table containing customer credentials. Trial Tr. 122:1-10. The logs showed the intruder's use of the madnez malware, which Formspring founder Ade Olonoh testified would not be used for legitimate Formspring business. Exh. 19; Trial Tr. 124:9-24. John Sanders's testimony explained how he was likely compromised. He was using a password manager at the time, and stored the password manager database file in his Dropbox account. Trial Tr. 67:8-68:5. In July or August 2012, Dropbox told Mr. Sanders that his Dropbox account had been accessed by a Russian IP. Trial Tr. 68:13-70:8.

Overall, the evidence showed important similarities between all three charged intrusions indicating that the same person was likely responsible. In addition, the evidence from LinkedIn led to the identification of chinabig01@gmail.com, which also linked all three intrusions. In August 2012, the computer with one of the two suspect browser cookies created a LinkedIn account for "Jammiro Quatro" In addition to using this unusual name, the person who created the account did not list a job title and had no connections. Exh. 32A. The login history for the account showed access from IP addresses in Russia and the sputnik user agent string. Exh. 32A. Cory Louie testified that Dropbox had also associated the chinabig01@gmail.com email address with the Dropbox intrusion. Trial Tr. 95:14—24. The name on the Dropbox account was "Jammis Gurus," which was similar to Jammiro Quatro. Exhs. 3C, 38. On June 13, 2012, the same day the Formspring intruder logged into Formspring's corporate network as John Sanders, chinabig01@gmail.com also created a Formspring account. Exh. 3E.

The Google search history for the chinabig01@gmail.com account (Exhs. 62A and 119) further correlated to the LinkedIn intrusion: the hacker got Nick Berry's SSH key on February 12, 2012; on February 18, 2012, chinabig01@gmail.com searched for "svn ssh key" "oracle export" and "oracle export utility;" Bruno Connelly testified that "Oracle is the software that we used at the time to store the login information among other things" (Trial Tr. 57:21-22); on June 6, 2012, the day after dwdm posted some of the LinkedIn data on insidepro.com, chinabig01@gmail.com searched for dwdm and visited the insidepro site; and the next day, chinabig01@gmail.com searched for "collision at md5" in Russian. MD5 is a hashing method.

Overlap between IP addresses used in connection with the intrusions and with accessing the various chinabig01@gmail.com accounts also showed that the same person who controlled

chinabig01@gmail.com was responsible for the intrusions. For example, Exhibit 142A showed that the Russian IP address, 178.176.33.207, was used to log in to both the chinabig01@gmail.com Dropbox account and Tom Weigand's Dropbox corporate account on May 27, 2012. Ex 19A showed that the IP address 178.177.28.0 was used within approximately sixteen hours to log in as LinkedIn member P. Minkov, log on to the corporate Dropbox system as tony@dropbox.com, and log into the Formspring corporate system as John Sanders. This showed beyond any reasonable doubt that chinabig01@gmail.com was responsible for the attacks on LinkedIn, Dropbox, and Formspring.

To further emphasize that the common methods of operation showed that the same person had committed the three charged intrusions and that person controlled chinabig01@gmail.com, the government also introduced evidence that chinabig01@gmail.com was responsible for a fourth, uncharged, intrusion in July 2013 at a company called Automattic, the parent of WordPress, which allows people to create and display web pages, including blogs. The Automattic intrusion involved login activity for Automattic employees that was very similar to the anomalous activity identified at LinkedIn, Dropbox, and Formspring; their accounts were accessed from Russian IP addresses and those IP addresses overlapped with activity by chinabig01@gmail.com. Trial Tr. 525:7-532-6. The logs showed that, on multiple occasions, at the same time the device assigned one IP address was accessing an Automattic computer without authorization, it was also logging into the chinabig01@gmail.com account at Google. Exh. 17A. The logs also showed use of "madnezz.php" – almost identical to the name of the malware used to attack Nick Berry and Formspring. Exh. 17; Trial Tr. 564:22-565:3. The chinabig01@gmail.com search history also links to the Automattic intrusion in two ways, just as it linked to the LinkedIn intrusion. For example, in the English search history there are searches for the names of Automattic employees such as "Ashish Shukla Automattic" at the time of the Automattic intrusion. Exh. 62A. In the Russian search history there was a search for "mysql fetch from 2 tables" a reference to a mysql database. Exh. 119; Trial Tr. 64:10.

The United States introduced significant evidence that defendant controlled chinabig01@gmail.com and therefore committed the charged intrusions. That evidence is organized into a chain – what the government described in closing as a "trail of digital breadcrumbs." Special Agent Miller testified that he investigated chinabig01@gmail.com to see how it connected to other electronic

accounts. Trial Tr. 481:4-10. He identified an account created at Afraid.org for chinabig01@gmail.com on November 8, 2012. Trial Tr.481:11-21. The Afraid.org records showed that the chinabig01@gmail.com account was associated with the Sputnik user agent string, the Russian language, and the username and password zopaqwe1. Exh. 45. Special Agent Miller also found that chinabig01@gmail.com had been used to create an account at vimeo.com on July 17, 2013. Trial Tr. 484:4-10. It had the user name "Uarebeenhacked" and IP address records that overlapped with the Automattic intrusion. Exhs. 17A, 113. Referring back to the Afraid.org records, Special Agent Miller followed the Zopqwe1 user name. He found that there was an account at the gaming site Kongregate with the username zopaqwe1 associated with the Russian Federation. Trial Tr. 517:1-10. The account records showed that the account owner had made credit card purchases through Kongregate in July 2012 in the name Jammis Tom, which sounds very similar to both the chinabig01@gmail.com LinkedIn alias Jammiro Quatro and the chinabig01@gmail.com Dropbox alias Jammis Gurus used in the summer of 2012. Exh. 48. In addition, the Kongregate account listed a different email address: r00talka@mail.ru.

Special Agent Miller testified that mail.ru was a Russian email provider, but that he found an account "r00talka@gmail.com" at Google and obtained records for that account. Trial Tr. 592:7-20. The search history and content for that account (there were no IP address login records) linked it to chinabig01@gmail.com and to defendant. Both accounts searched for information related to the LinkedIn hack in June 2012. Exhs. 62A and 143F. Both accounts contained searches for Kantemirovskaya Street, such as a search for a nearby address (not the defendant's) or for "dentistry Kantemirovskaya." Exhs. 119, 143F. Overall, the searches evinced similar interests: potential vulnerabilities, user data, shells, and php programs. Another key link between chinabig01@gmail.com and r00talka@gmail.com was the Kongregate account discussed above. Chinabig01@gmail.com set up an account at Afraid using zopaqwe1; r00talka@mail.ru set up an account at Kongregate using zopaqwe1. The Kongregate records included a credit card number ending in 0405 data that was also referenced in purchase confirmations sent to r00talka@gmail.com, all in August 2012. Exhs. 48, 143D. Messages in the r00talka@gmail.com account were addressed to "china china" just as messages in chinabig01@gmail.com were addressed to chinabig01 chinabig01. Exhs. 3A, 143D. There was also an IP overlap in July 2012 between the Kongregate data and the Dropbox intrusion, which showed that the

Kongregate account was controlled by the same person responsible for the Dropbox hack. Exh. 142A.

Most significantly, the r00talka@gmail.com account linked directly to defendant through his VKontakte ("VK") social media profile. Special Agent Miller testified that VK was the Russian equivalent of Facebook. Trial Tr. 510:2-3. The r00talka@gmail.com account contained automated notifications from VK, including text and photos, such as defendant messaging with his girlfriend Anna:

Exh. 143K. The account also contained notifications for messages posted to defendant's VK account by his brother Mikhail. The defendant was still in contact with both Anna Shvedova and Mikhail Nikulin at the time of the trial. Exhs. 148 and 150. The account name in the notifications was sometimes "Top Man" and sometimes "Evgeny Kantemirovsky." One of the messages sent to defendant included a post that refers to his living on Kantemirovskaya Street. Only the defendant would have wanted to receive these notifications. By proving that r00talka@gmail.com was defendant, the government proved, through the trail of digital breadcrumbs, that defendant was chinabig01@gmail.com and therefore responsible for the intrusions.

The United States also proved that defendant worked with co-conspirators to traffic Formspring data that he had stolen. Special Agent Miller testified there are specialized roles for those involved in the sale of stolen data online: hackers who break into websites and steal data; brokers who help facilitate the sale of the stolen data; buyers who buy the stolen data; "bruters" who are individuals who try to "brute force" crack or decrypt the stolen passwords; and "cash-outs" who help turn stolen data into real money. In this case, defendant was the hacker – he obtained the Formspring data in June 2012. Slavuti4 was the bruter – on July 6, 2012, he posted the hashes on insidepro.com looking for help. Exh. 6. Nikita Kislitsin was the broker – at Alexsey Belan's insistence, he contacted Nikulin and reported back to Belan that the database Nikulin was selling was Formspring. Exh. 120. Belan confirmed after

investigating that the bruter and not defendant was the one who posted the Formspring hashes on insidepro.com. Mehmet Sozen or "Rais" was the buyer. Kislitsin offered to sell the Formspring database to Sozen. Exh. 22A. Kislitsin confirmed that he had multiple fields for the database, including name and email, not just the hashes that had been posted to insidepro.com, meaning he must have gotten the data from the person who stole it. Sozen requested and took a sample of the Formspring data (Exh. 128) and then agreed to pay $7,200 for it. Ex. 22A. Oleg Tolstikh was the cash out – Sozen sent Tolstikh two wires through Western Union for the full amount. Exhs. 22A, 25A. The only reasonable inference from this evidence was that because Defendant committed the Formspring hack, he was the one that Kislitsin got the data from. There was no evidence in the case that anyone else had Formspring data at the time. There was evidence linking Kislitsin, defendant, and Tolstikh – the hotel video discussed above. Exh. 74.

The NCN ISP records from Russia discussed above directly show that defendant was responsible for the intrusion into LinkedIn and therefore for all of the charged conduct. Those records showed that defendant was the person assigned the IP address ending in .239 on March 3 and 4, 2012, at an address on Kantemirovskaya Street:

Connection (on the date and at the time indicated in the request from the dynamic **IP address 178.140.105.239**) was established from the workstation of the network user of OAO National Cable Networks [Russian abbreviated name OAO NKS]

FULL NAME	Nikulin Evgeny Alexandrovich
ADDRESS	Moscow, rayion Tsaritsyno, Kantemirovskaya ulitsa, d. 17 kop. 1, p. 6, et. 5, kv. 250
PHONE	(909) 690-90-25
PASSPORT	45 09 486514
Additional Information	MAC 0025643a6f57 Contract No. 5645935, personal account 3121515

Exh. 85A. First, Kantemirovskaya Street appeared repeatedly in the evidence, including the search history for both chinabig01@gmail.com and r00talka@gmail.com. Second, the .239 IP address was one among several Russian IP addresses used during the LinkedIn hack, but was the most important because it was used for that extraordinarily long VPN connection of two days, seven hours, eighteen minutes, and six seconds in which over three GB of data were transferred. Exhs. 26B, 33. A connection of that

length and volume would require the kind of stability that defendant would have been able to assure only from a connection he controlled. Defense counsel raised the issue during cross examinations that proxy servers can mask an IP address, but, as Mr. Krishnan confirmed, a proxy server was a second connection that needed to stay stable in order to avoid disrupting a VPN connection. Trial Tr. 290:13-19; 311:12-312:16. To extract the millions of LinkedIn user names and hashed passwords that he stole, defendant would have used the stable connection he trusted – his own.

In addition to the "hotel videos" discussed above, the Skype chats saved on Ieremenko's computer between Ieremenko – using the Skype account vaiobro and screen name Sergey Shalyapin and defendant – using the Skype account dex.007 and screen name Evgeny Lomovitch were significant evidence tying defendant to the intrusions. The government's Russian linguist, Andre Romanenko, testified that Lomovich looked like a nickname that he would translate as "Hackenberg" or "Breakovitch." He explained that the root of the word meant "break or breaking" and that "lom" translated to crowbar in English. Trial Tr. 359:16-360:5. In the chats at Exhibit 76B it was clear that defendant was Lomovich for several reasons: he talked about trouble with his girlfriend Anna; on October 18, 2012, Ieremenko wished Lomovich a happy birthday and said to give yourself a present "tomorrow," meaning October 18, 2012; defendant's birthday is October 19, 1987; defendant talked about getting a watch for up to $25,000 for 25 years, which is how old he would have been in 2012.

The messages in Exhibit 76B also showed that defendant had the LinkedIn data in October 2012, before it was posted publicly in 2016. Defendant, as Lomovich, sent Ieremenko LinkedIn members' email addresses and hashed passwords, in response to Ieremenko's requests by LinkedIn member numbers. According to the time stamps, it took defendant only two minutes to turn around the emails and password hashes. He clearly had the stolen data at his fingertips. The two also discuss C99 madshells – the type of malware defendant used to attack Nick Berry, Formspring, and Automattic. This showed that, not only did defendant have the stolen data, but he was familiar with the malware used to obtain it.

Finally, there were IP addresses associated with the dex.007/Lomovich activity that Special Agent Miller recovered from the Ieremenko drive that proved defendant was responsible for the intrusions. Exhibit 19B showed that the same person – defendant – accessed Formspring's servers, two

different LinkedIn accounts, a Dropbox employee account, and chatted as dex.007/Lomovich with Ieremenko over the span of two days:

2310	06/14/2012 18:41:26	178.177.28.0	GET /favicon.ico HTTP/1.1 401 290	Formspring - ssl_access_log.4
2311	06/15/2012 01:11:44	178.177.28.0	8aa74797-0a46-4fac-801e-9547ddda7082	LinkedIn Consumer Account Login - Member 6879748
2312	06/16/2012 14:17:06	178.177.28.0	8aa74797-0a46-4fac-801e-9547ddda7082	LinkedIn Consumer Account Login - Member 6879748
2313	06/16/2012 14:19:00	178.177.28.0	Access Activity	Dropbox Employee - tony@dropbox.com
2314	06/16/2012 14:19:00	178.177.28.0	Access Activity	Dropbox Employee - tony@dropbox.com
2315	06/16/2012 14:27:44	178.177.28.0	8aa74797-0a46-4fac-801e-9547ddda7082	LinkedIn Consumer Account Login - Member 15779395
2316	06/16/2012 18:17:39	178.177.28.0	IP assigned to dex.007 during Skype chat with vaiobro	dex.007 Skype Data from Ieremenko Computer
2317	06/17/2012 18:55:57	178.177.28.0	8aa74797-0a46-4fac-801e-9547ddda7082	LinkedIn Consumer Account Login - Member 15779395
2318	06/17/2012 22:02:50	178.177.28.0	sshd[28085]: Accepted password for jsanders from 178.177.28.0 port 61364 ssh2	Formspring - secure.3
2319	06/17/2012 22:04:58	178.177.28.0	sshd[28449]: Accepted password for jsanders from 178.177.28.0 port 61369 ssh2	Formspring - secure.3
2320	06/17/2012 22:05:49	178.177.28.0	sshd[28751]: Accepted password for jsanders from 178.177.28.0 port 61373 ssh2	Formspring - secure.3
2321	06/17/2012 22:11:54	178.177.28.0	sshd[30228]: Accepted password for jsanders from 178.177.28.0 port 61454 ssh2	Formspring - secure.3
2322	06/17/2012 22:12:26	178.177.28.0	sshd[30384]: Accepted password for jsanders from 178.177.28.0 port 61455 ssh2	Formspring - secure.3

Exh. 19B.

Finally, as discussed above, there were defendant's own words in the recorded calls, including his statement to Anna: "I hack websites 24/7. I hacked." Exh. 89.

The trail of digital breadcrumbs that the government laid out for the jury established that defendant committed the charged crimes. Defendant did not directly challenge this evidence, almost all of which came in without objection, and he did not present any cohesive alternative. Instead he argued that the jury should disregard the actual evidence and engage in speculation about which other Russian hacker the FBI should have investigated and what nefarious cover-up the Russian government could have concocted back in 2012 to frame defendant. But there was no other hacker and there was no cover-up. The evidence, including direct evidence from defendant himself, established his guilt.

C. The Jury Did Not Misunderstand the Evidence

Defendant claims in his brief that "[i]n addition to the grounds previously set forth, the jury's verdict clearly manifested a Mis-understanding of the evidence." Defendant offers no basis for this argument, and there is no reason for the Court to come to that conclusion. The government clearly explained the significance of the evidence at closing, as described above. Defendant was permitted to question Special Agent Miller about Bogachev, other Russian cyber criminals, the FBI investigation of defendant, and the far-fetched notion that the evidence pointing to defendant was all a Russian government cover-up.[14] Defense counsel then presented those arguments at closing. In coming to its

[14] Defense counsel also cross examined U.S. Secret Service Special Agent Richard LaTulip at length about Oleksandr Ieremenko's criminal hacking activities and the investigation of those activities.

guilty verdicts, the jury resoundingly rejected all of those unfounded attacks on the government's case, but there is no reason to think they misunderstood them. The jury deliberated for over six hours. The jury's question about the aggravating factors for one of the counts indicated that they were paying close attention to the evidence, the jury instructions, and the special verdict form. ECF 262. The Court should not disturb the jury's hard work based on mere speculation.

CONCLUSION

For all the reasons stated above, the Court should deny defendant's motion for acquittal pursuant to Rule 29 and deny defendant's motion for a new trial pursuant to Rule 33.

DATED: September 8, 2020

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s/
MICHELLE J. KANE
KATHERINE L. WAWRZYNIAK
Assistant United States Attorneys

Trial Tr. 344:17-349:18.